Safer use of technology

New technologies, new opportunities

New technologies offer tremendous opportunities to reach, communicate, evangelize and engage with those involved in the Catholic Church and those in our communities who may have an interest in the church. The internet, mobile phones, social networking and other interactive services have transformed the way in which we live.

New technologies, new risks

Along with the many benefits of modern communication technologies, there are risks. The anonymity and sense of distance inherent in online communication can make it easier for people to say things they would perhaps not say in the presence of somebody, and to feel less remorseful about online harm caused.

The online world makes it easier to engage in criminal offences and abuse. It enables easy creation of, access to, use and dissemination of pornographic and abusive images and videos, easy access to children and adults who are vulnerable for the purposes of grooming, ease of presenting as someone else and greater potential for online bullying and abuse.

The use of church computer equipment to store information

Diocesan or congregational policy and procedure on the use of its own computer equipment and the storage of information on personal computer equipment must be followed.

Electronic storage of records on computer equipment

Electronic storage of records is often considered to be preferable to paper storage because electronic records can be more easily accessed, searched and shared and version control can be easily managed. The disadvantages include risks relating to changes in software and formats perhaps rendering electronic documents unreadable in the future.

Electronic safeguarding records, like paper records, should:

- Be held in protected folders with restricted access, to ensure that only authorised individuals can access them;
- Be kept in accordance with the record retention schedule.

Creating and managing church-related websites and social media pages

Websites or social media profile pages are useful means to engage large groups of young people. The following are recommended guidelines to promote safety online:

- Any church-based Website or Social Media Profile should be approved by the parish and should be disclosed to the diocese;
- Where there is user-generated content, the site should be moderated/ administered by a minimum of two adults;
- Personal sites should not be used for diocesan or parish programs; separate sites should be created for these;
- Passwords and names of sites should be registered in an encrypted document in a central location in the parish and/or diocese as appropriate. More than one adult should have access to this information.

Accessibility of websites and social media pages
Websites need to be accessible to all and adjustments could include functions that change, contrast, text size or offer an audible alternative when viewing web pages.

Examples of such adjustments can be found at the **DisabledGo website**;

Tiresias.org – also gives advice on how to create a website that is accessible to all.

Access to the internet

Where children, young people and adults have access to the internet using church computers, other electronic devices and WIFI as part of Church activities, the event leader has a duty to ensure that:

- Use of the equipment and WIFI is supervised and/or monitored;
- Measures are in place to ensure that the likelihood of accessing inappropriate materials is reduced e.g. firewalls, parental controls and software to filter out internet material.

Social media and social networking

The internet has evolved to become an increasingly dynamic and interactive medium led by social networking services. The convergence of technical and communication platforms means that users can now interact with each other across multiple platforms and devices, such as mobile phones, games consoles, watches and PCs (laptops, notebooks, tablets etc.).

Social media includes any site or forum that enables sharing of any user-generated content. These services are very popular with children and young people and bring together pre-existing interactive technologies and tools (e.g. email, messaging, chat, blogs, photographs, music, videos, gaming, discussion forums) in a single service through for example Facebook, Twitter, Instagram, WhatsApp,

Snapchat and live messaging services such as Facetime, Duo and Skype, and so on. It is the way in which these different technologies are used that makes them 'social'.

Good practice in relation to social networking:

- Government guidelines recommend children under 13 years should not be using social media;
- All users should be made aware that their personal details e.g. last name, address, school, passwords, e-mail address and telephone numbers are private and should not be disclosed unless approval is given by the event leader;
- All users should be made aware that they should never send images of themselves or others and should be wary of people misrepresenting themselves in chat rooms;
- All users should be aware that they should advise a leader about anything on line that makes them feel uncomfortable or concerns them;
- Children and young people should be advised to always tell an adult they trust about communications that make them feel uncomfortable or where they have been asked to keep communication secret;
- Children and young people should be made aware that they should advise a leader and their parent or carer of a request to meet up with someone they have met on line, not to make plans to do so without alerting an adult and never to go alone to such planned meetings;
- Children and young people should be advised of a code of conduct for using chat rooms.

'CHAT' is a simple code that can be used for remembering some rules around the use of the internet and social media.

C	= Careful - People online might not always be who they say they are.
H	= Hang - Hang on to your personal information. Never give out your home address or other information.
A	= Arranging - Arranging to meet can be dangerous. Never arrange to meet someone unless you are sure who they are.
T	= Tell - Tell your friends or an adult if you find something that makes you feel uncomfortable.

The use of social networking for communication with children and young people

The diocesan, congregational or organizational policy and procedure on the use of social networking for communication with children and young people must be followed.

In the absence of a local policy and procedure the following good practice guidance can be followed.

- If a group, parish or other body decides that the most effective way of communicating with children or young people is via a social networking site, it is advisable to set up a custom account in the name of that group, parish or body. How the media is used should also be made explicit to children and young people, and permission must be sought from parents.
- Social media sanctioned by church organisations or personnel should be moderated by at least one adult familiar with Safeguarding procedures, and a minimum of two adults in total;
- Parents should approve and have access to all sanctioned social networking that is directed at children and young people;
- Children or young people should not be online for any other reason than the specific ministry for which parental consent was obtained;
- All communication, including online, between an adult and a child or young person should take place via the most public means of communication appropriate without jeopardising duties to protect data under the General Data Protection Regulation (EU) 2016/679;
- For matters that are sensitive or private, online communication should be avoided due to the possibility of misunderstanding and, if used, parents should be included.

Personal social networking accounts

The diocesan, congregational or organizational policy and procedure on the use of personal social networking accounts must be followed.

In the absence of a local policy and procedure the following good practice guidance can be followed.

Many clergy, religious, lay persons, employed staff and volunteers have a personal online social networking presence via social media platforms, personal blogs and websites. As a member of the Church, personal social networking (e.g. Twitter or Facebook) should always reflect Catholic values and should contain content that is universally appropriate to any possible user. Whether public or private, all individuals should understand that they are witnessing to the faith through all of their social networking and as such, personal views should be cited as such to avoid misunderstandings.

Although there may be reasonable overlap between the personal and spiritual realms in communications between adults (with full capacity) within the Church, this is never the case with children, young people or adults at risk.

It is never appropriate to use personal social media accounts, phone numbers or email addresses to contact children and young people without parental consent, or with adults who lack capacity to give their consent.

It is not appropriate to send or accept 'friend requests' from children, young people or adults who lack capacity to consent from personal social media accounts.

The strictest of privacy settings should be activated on all personal social media accounts and individuals must take personal responsibility to ensure that their content is appropriate to those that can see it e.g. language, jokes, opinions.

Church website and social media monitoring and reporting

- Dioceses, parishes and religious congregations should appoint suitably skilled adults to monitor the content of their websites and take action to remove offending material;
- Any discovery of inappropriate use (of a safeguarding nature) of social networking sites, computers, email or texting should be reported to the parish Safeguarding Representative or Safeguarding Coordinator who will report to the relevant person within the diocese, parish or religious congregation;
- Church personnel must report unofficial sites that carry the diocesan, parish or religious congregation's logo to the Diocesan Communications Office, Parish Priest or relevant person within the religious congregation. It is important that the owner of the site is able to protect its identity and prevent unwanted publications. Any misinformation found on a site, such as Wikipedia, should also be reported to the Communications Officer or relevant role;
- Any forum that includes user-generated content should be moderated on a regular basis to prevent libellous, rude or inappropriate remarks so that the information can be removed;
- Consider adding the CEOP help button to your site. The CEOP help button gives access to help on viruses, hacking, online bullying and enables reporting of people acting inappropriately online www.ceop.police.uk.

Administrators and Moderators

The diocesan, congregational or organizational policy and procedure in respect of administration and moderation must be followed.

In the absence of a local policy and procedure the following good practice guidance can be followed.

Adults moderating sites and adding user-generated content should take care:

- To appreciate that even personal communication by church personnel reflects the Church;
- To write in the first person;

- Not to claim to represent the official position of the organisation or the teachings of the Church, unless authorised to do so;
- To identify themselves with real, full names;
- Not to divulge confidential information about others;
- To avoid posting personal, political or negative content online;
- To ensure that text and photographs posted are in the public domain and not subject to copyright infringement;
- To not cite others, post photographs or videos of them, link to their material, without their explicit permission; once posted, material often becomes property of the site;
- To practice Catholic teaching and morals at all times;
- To always report any form of bullying, trolling or libel to the diocese, parish or religious congregation;
- To always report any concerns about any inappropriate behaviour online;
- To always report any suspected online grooming.

The use of email and texting (SMS)

The diocesan, congregational or organizational policy and procedure on the use of email and texting must be followed.

In the absence of a local policy and procedure the following good practice guidance can be followed.

The benefits of email and text messaging (Short Message Service - SMS)
Emailing and SMS are a widely accepted and attractive means for communication that people of all ages rely upon. Benefits of communication by email and SMS include quick and easy communication without delays and reduced postage costs.

Email and SMS can be helpfully used in relation to Church activities to:

- Send quick messages to individuals such as reminders about or changes of arrangements for activities;
- Broadcast the same message to a wide-ranging audience such as promotion of an event.

<u>Agreeing the use of SMS</u>
The need or benefit of using email and SMS and approval of its use should be agreed with the leader of the Church group or activity. The approval should be documented along with the following:

- Identification of the need or justification for the use of email and SMS;
- Identification of when email and SMS will be used;
- The agreement to the use of the service by its intended recipients;
- Clear identification of the associated risks and of the means by which these risks are managed;
- Storage of messages sent and received.

Consent

Written consent must gained from adults at risk or the parents of a child or young person (up to 18 years of age) and for 16 and 17 year olds, the young person's consent should also be sought, prior to the commencement of email and SMS messaging taking place.

When written consent is being sought the potential benefits and risks should be explained before deciding on whether or not to receive email and SMS communication.

Consent to be contacted by email and SMS can be withdrawn at any time and must be implemented without delay.

Risks

The following risks must always be taken into account:

- Emails or SMS not reaching the intended recipient;
- Content sent in haste that cannot be retracted;
- Storage of content as 'records';
- Information not being sent securely via the internet.

Safer practice

Using Emails and SMS to communicate with children, young people and adults at risk should be done using an organisational account and organisational equipment. It is not recommended that personal telephones or accounts be used for communicating with children and young people or adults at risk.

A generic email address or telephone number associated with the role in question (voluntary or not) maintains appropriate boundaries.

Where more than one leader or helper needs to communicate with group members, it might be appropriate to set up a generic shared email account and have a shared mobile telephone. The benefits of this are that:

- Communications can be easily reviewed by other leaders or helpers in the event of enquiries;
- The need for action on any matter can be easily shared and delegated;
- Communications can be picked up in the event of sickness or other absence;
- All correspondence and data is stored securely in one place.

Email and SMS should not be used to transmit person identifiable information, confidential or other sensitive information.

Those to be included on group email addresses must give their consent to be included in group communications.

The BCC field should be used for group emails to avoid other recipients receiving the contact details of other recipients.

When sending messages, emails or texts to young people, parents another group leader or helper should be copied into all communication. All communications should be strictly regarding a specific Church activity and not be personal conversations, contain pictures, jokes or anything of a personal nature.

Emails or texts from young people other than those directly related to your role within the Church or the activity you are concerned with should not be responded to.
The Safeguarding Representative or Safeguarding Coordinator should be advised if somebody receives any inappropriate texts, images or emails.

Copies of all texts, WhatsApp chats, personal messages and emails should be kept on file.

Newsletter Mailing Clients

A potential way of managing bulk communications and protecting personal data is to use a newsletter mailing client.

Useful links and resources for internet safety

- The UK Council for Child Internet Safety (UKCCIS) is a voluntary organisation chaired by Ministers from the Department for Education and the Home Office. UKCCIS brings together over 180 organisations and individuals from government, industry, law enforcement, academia, charities and parenting groups. Some of the organisations UKCCIS works with include: Cisco, Apple, Sony, Research in Motion, the four largest internet service providers, Facebook and Microsoft;
- The Child Exploitation and Online Protection Centre (CEOP) has numerous resources for parents and carers and children using the internet; there are several video tutorials on the THINKUKNOW site which is part of CEOP;
- Lucy Faithful Foundation is a registered child protection charity which works to prevent child sexual abuse. It runs 'Stop It Now!' and 'Parents Protect:
    - Stop It Now! reaches out to adults concerned about their own behaviour towards children, or that of someone they know, as well as professionals, survivors and protective adults. Stop It Now! runs a Freephone confidential helpline.
    - 'Parents Protect' is a site to help parents, carers and other protective adults with information and advice to help them prevent child sexual abuse.
- Catholic Youth Work has detailed guidelines on the use of social networking sites;
- Internet Matters gives advice on parental controls and is a great way of preventing children accessing unsuitable content online;

- Childnet International is a multi-lingual resource site which has a guide on protecting your privacy on 'Facebook';
- The NSPCC has useful resources for keeping children safe online including sections on Cyberbullying and Sexting. Reporting and Monitoring.